

CCUK Best Practice Guide: Know your traffic - Monitoring for fraudulent calling patterns

May 2026

Introduction

Scams, fraud and nuisance calls are all serious problems that are at the top of the political and regulatory agenda. There is no single solution to resolve the problem, however there are a number of tactics available to help minimise it. These tactics range from proactive measures (such as call blocking and caller verification) to reactive measures (including reporting incidents of fraud to the relevant authority and retrospectively blocking service).

The following guidance is created for CCUK members to help you understand your obligations towards monitoring your customers calling patterns and knowing what they are using your services for. This is a critical step towards disrupting bad actors who may have slipped through your due diligence process, alerting you to issues so you can take steps to cease service and disrupt the scam or fraud.

This guidance is broad in order to cover members of all sizes with a variety of service offerings. It is for you to decide which recommendations are suitable and proportionate for you to carry out with your own customer base. We strongly recommend that you document your own processes and procedures so that you can demonstrate your compliance with Ofcom's requirements.

This guide to monitoring for suspect calling patterns should not be viewed in isolation, when considering your processes for monitoring for scam calls and fraudulent use, we also recommend reading the other related best practice guides that are available to download from our members area such as 'Preventing Misuse of Sub-Allocated and Assigned Numbers'

.

Know Your Traffic:

Monitoring and understanding the voice traffic using your service is important for many reasons and this document is intended to deal with the importance of monitoring for reasons of regulatory compliance. Tools and systems to monitor traffic patterns may already be in place if you are using them for monitoring for commercial aspects.

The first thing is to consider what normal traffic looks like to you – based on your ideal customer profile. This will help you make decisions around what a safe call traffic profile and risky call traffic profile looks like for your business so that you can monitor accordingly.

High risk high risk traffic – can be broadly categorised into:

“Hacked switchboard” – where equipment is compromised and unauthorised calls are made, often to expensive or revenue generating destinations. Further guidance on these issues can be found in the Members Wiki 'Recommendations for device provisioning security'.

“Scam calls – predatory/unwanted marketing”. These are the type of calls that often result in fraudulent payments being made by victims to scammers. The theme of the scam often changes depending on what issues of concern are playing out in the public narrative, but the

metrics and calling patterns often remain similar enough to be able to identify the calls alongside KYC measures.

Proactive steps:

Caller ID (CLI) screening: CLIs should be screened for validity and in line with all current regulatory requirements for the use of CLI.

CPs can read more information about obligations for CLI validity in General Condition G6 and can find CCUK guidance in the Members Wiki 'UK Caller Line Identity Guidance' but the basic checks suggested below cover most of the current requirements on CPs.

Basic validity checks include verifying the CLI has the correct number of digits and is in a suitable format. A valid UK CLI is defined as "a number that is designated as a 'telephone number available for allocation' in the Numbering Plan and be shown as allocated in the national Numbering Scheme".

As well as being from valid ranges, all Caller IDs presented should be live and be able to be dialled back, i.e. should a called party return a call it must be clear from any IVR or agent response who had called them.

Calls that are originated outside of the UK (or Crown Dependencies) are prohibited from using a UK Network or Presentation number, except in a limited set of circumstances. CPs should take steps to block these calls, or understand why an exception may apply to calls so that calls can legitimately progress. Reporting on the originator and quantity of calls that get blocked under this regulation is a useful KYT metric, as you may be able to identify the source of unwanted calls on your network.

Screening against Do Not Originate (DNO) list:

The DNO list is collated and maintained by Ofcom and consists of numbers that businesses and organisations have submitted to the list, as they will never be used by that business or organisation to originate outgoing calls. Telecoms providers must screen calls against this list and any outgoing calls appearing to originate with numbers on the DNO list should be blocked as they are clearly spoofed and are not genuine calls from that organisation. Customers originating calls that are blocked by DNO screening require further investigation.

You can find out more information on the DNO list here:

<https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/do-not-originate/>

Screening against Telephone Preference Service (TPS) list:

The TPS is a 'Do Not Call' register which allows people and businesses to register their numbers in order to opt out of unsolicited live sales and marketing calls.

If your customer is making sales and marketing calls and subscribes to TPS screening services via your service, a higher than usual % of calls being blocked will require further investigation.

Ongoing monitoring.

Sudden change in call traffic levels:

An unexpected change in a clients normal traffic patterns – whether increase or decrease – is a flag for further investigation.

For example – a sudden, large or un-forecasted increase in traffic routed via your service from a dialler type customer is often a sign that another CP has denied them routing and they have needed to find a new service provider for these calls.

Short duration calls:

Once you understand what your normal or ideal call length looks like you can monitor for traffic outside that parameter.

It is widely accepted that ‘conversational’ traffic has an average call duration of 60+ seconds, but once you understand your own ideal traffic and your customers use cases, you can understand what your normal looks like.

Accounts with an average call duration of less than your parameter may indicate the type of calling which will need closer monitoring for compliance with the Privacy and Electronic Communications

Regulations (PECR)

This is where the KYC comes into play alongside the KYT, as it will help you understand the use cases for very short calling; appointment reminder calls, sole worker welfare check calls, and so on all have valid use cases for being short in duration.

Answer Machine Detection or AMD – software used by dialler providers to reduce the time spent on calls that do not reach a live person. If you see a high % of calls lasting 1 second or less, this account may benefit from closer KYC to understand the nature of the calls being made.

Similarly, a high % of calls lasting only a few seconds suggests that the far end does not wish to engage with the calling party, so high volumes of especially short calls like this may be a useful metric to monitor.

Low Answer Seize Ratio (ASR): Low amounts of connected calls could be for many reasons. These could include the far end simply not answering (i.e. ringing, but no answer), a far end network may have blocked calls due to multiple reports of unwanted calls, or dialling list may be old/outdated with a lot of out of service numbers in – having outdated or poorly managed dialling lists often goes hand in hand with scam calling.

For normal conversational calling, an ASR should be 65% or higher and anything with a lower ASR may indicate the type of calling which needs closer monitoring.

Wardialling patterns: This is normally the more primitive dialling pattern of an unsophisticated scam caller trying to hit on a valid number – despite the progress and intelligence of scammers these days, these patterns are still worth watching out for. In their most simplistic form this means a dialler is progressively dialling through all the numbers in a range, like 0118 123 4567, 0118 123 4568, 0118 123 4569 and so on.

Hangup cause: You could rationally consider that normal conversational calling ends half by the caller and half by the callee end – i.e. 50% of the dialled parties hanging up and 50% of the callers hanging up. High volume outbound calling with a much greater % of calls hung up by the called party is a metric you may wish to consider monitoring, as the implication would be that the calling party is making a lot of calls that the called parties do not wish to participate in.

Experienced eyes: Do not under estimate the value of a member of staff who develops a skill for effectively identifying a suspect calling pattern. KYC and KYT are incredibly useful tools, but

having colleagues who are empowered to review traffic patterns to investigate an instinct is of considerable value to a conscientious telecoms provider.

Incidents of Misuse

Providers must also have a process in place to deal with non-compliance situations. We suggest that members document their process and what will trigger it and when it should be followed, again ensuring that all relevant employees are aware of the steps to be taken.

You should take the following steps to comply:

- Develop and maintain a process for handling incidents of suspect calling being identified, being sure to maintain records of any investigations you carry out.
- Ensure that you can be contacted quickly and easily to be notified of suspected misuse.
- Ensure you take appropriate action to investigate and resolve incidents of suspected misuse in a timely manner and relative to the severity of the incident.

It is up to you to weigh up the evidence and take “necessary and proportionate action”.

Evidence includes metrics from your own monitoring for troublesome call patterns and KYC, combined with complaints, CLIs appearing on warning lists and reports from law enforcement.

Once you have identified misuse via calling patterns, if these cannot be adequately explained via KYC, you must take steps to prevent further potential misuse as far as reasonably possible.

This might include invoking contract conditions on your customer and blocking calls. The action taken should be proportionate to the evidence and the risk posed.

Affected consumers should be supported as appropriate, and you must cooperate with Ofcom and other relevant organisations. If the incident involves numbers sub-allocated from other networks used as presentation numbers, you should also consider informing the range holder of any incident.

If you have evidence of criminal activity, notify law enforcement. You may also consider reporting to Report Fraud online, or call 0300 123 2040.

In addition, we encourage you to report proven or potential criminal behaviour to the National Trading Standards Scams Team who will anonymise the source and share the data back to other members, helping reduce the risk that the scam will simply continue via another provider. You can email the Scams Team on scamsteamadmin@surreycc.gov.uk. For more details about this scheme please visit the Members Wiki for ‘Sharing information to prevent, detect and report fraud’ guidance.